Главе Лямбирского муниципального района Республики Мордовия

Голову Ю.И.

18.12.2020 № 22/2-1-2020

Уважаемый Юрий Иванович!

Направляю для использования в работе и опубликования на официальном сайте муниципального района в разделе «Прокуратура Лямбирского района» разъяснения: «Об уголовной ответственности за хищение электронных средств платежа», «Профилактика мошенничества с банковскими картами».

Информацию об опубликовании прошу направить в прокуратуру района.

Прокурор района

старший советник юстиции С.В. Сидоров

Кисняшкина А.И., 2-90-56

Об уголовной ответственности за хищение электронных средств платежа

Хищение электронных денежных средств является одним из распространенных преступлений. С целью борьбы с указанным преступным проявлением Федеральным законом от 23.04.2018 № 111-ФЗ часть 3 статьи 158 УК РФ дополнена пунктом «г», предусматривающим более строгую ответственность за тайное хищение, совершенное с банковского счета, а также в отношении электронных денежных средств. Этим же законом введена статья 159.3 УК РФ, выделившая мошенничество с использованием электронных средств платежа в отдельный состав преступления.

Квалификация деяния при хищении денежных средств с банковских карт граждан зависит от способа завладения ими.

Согласно постановлению Пленума Верховного Суда Российской Федерации от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате», хищение денежных средств путем использования заранее похищенной или поддельной платежной карты, если выдача наличных денежных средств была произведена посредством банкомата, следует квалифицировать как кражу. Аналогичным образом необходимо квалифицировать и действия лица, похитившего безналичные денежные средства, воспользовавшись необходимой для доступа к ним конфиденциальной информацией, в том числе переданной самим держателем платежной карты.

Например, уголовной ответственности за кражу подлежат злоумышленники, снявшие с чужой банковской карты без разрешения ее владельца наличные денежные средства посредством использования банкоматов или терминалов самообслуживания. Таким же образом квалифицируются действия виновного лица при переводе денежных средств со счета потерпевшего на счет обвиняемого путем использования сервисов «Сбербанк онлайн», «Личный кабинет», «Мобильный банк», когда незаконному перечислению предшествует завладение телефоном потерпевшего, подключенного к соответствующим банковским сервисам.

В этом случае осужденному может быть назначено наказание в виде штрафа, принудительных работ либо лишения свободы.

Если для хищения денег виновное лицо использует обман или злоупотребление доверием, то данные действия квалифицируются по статье 159.3 УК РФ. Например, такое хищение может быть совершено путем сообщения сотруднику банка, магазина или иной организации заведомо ложных сведений о том, что карта принадлежит виновному на законных основаниях, либо путем умолчания о незаконном завладении ею. В частности, преступник может расплатиться картой в магазине, воспользовавшись технологией, позволяющей производить расчеты без введения ПИН-кода, выдавая себя за владельца карты.

За совершение преступления, предусмотренного статьей 159.3 УК РФ, законодателем предусмотрены штраф, обязательные работы, исправительные работы, ограничение свободы либо лишение свободы.

Профилактика мошенничества с банковскими картами

С развитием современных информационно-телекоммуникационных технологий представить жизнь современного человека без уже ставших привычными нам технических устройств, электронных средств платежа, невозможно. Их простота и доступность в использовании привлекают все большее и большее число пользователей. Наряду с этим не отстают от них и преступники, использующие современные технологии в своих криминальных целях.

Мошенники выдают себя за банковских работников, специалистов служб социальной защиты, вводя в заблуждение граждан, выясняют у них персональные данные, информацию о банковской карте/счете, используют полученные сведения в корыстных целях. При этом особенно уязвимыми являются пожилые люди и подростки. Распространение получила схема, когда по телефону собеседник представляется сотрудником банка, говорит о том, что сработала система безопасности, и в данный момент по карте клиента проводится подозрительная операция. Чтобы ее остановить, необходимо назвать, к примеру, кодовое слово или ПИН-код. В дальнейшем мошенники, применяя психологические манипуляции, давят на людей, стимулируют их к совершению определенных действий со счетом или карточкой, необходимых для похищения денежных средств. Зачастую гражданам на телефон присылают SMS-сообщения подобного содержания.

Очень популярны среди населения покупки в интернет-магазинах и на сайтах объявлений типа «Avito». При этом, нередко продавец просит перечислить ему аванс за товар либо его полную стоимость с карты на карту. После перевода мошенник, естественно, исчезает.

Прокуратура Лямбирского района просит соблюдать рекомендации гражданам:

1. Только мошенники могут запрашивать Ваш номер мобильного телефона и другую дополнительную информацию, помимо идентификатора, постоянного и одноразового паролей.

2. Только мошенники могут запрашивать пароли для отмены операций или шаблонов в «Сбербанк Онлайн». Если Вам предлагается ввести пароль для отмены или подтверждения операций, которые Вы НЕ совершали, то прекратите сеанс использования услуги и срочно обратитесь в банк.

3. Только при мошеннических операциях реквизиты Вашей операции не совпадают с реквизитами в полученном SMS-сообщении.

4. Только на мошеннических сайтах контактный телефон не соответствует официальным.

5. На мошеннических сайтах в адресной строке браузера отображаются цифры ip-адреса или любые домены кроме зарегистрированных доменных имен системы «Сбербанк-Онлайн».